Индивидуальный проект - 4

Использование nikto

Кузьмин Артем Дмитриевич

Содержание

1 Цель работы 4

2 Введение 5

2.1 Nikto: Описание 5

2.2 Полезные параметры и примеры 6

3 Выполнение лабораторной работы 7

3.1 Сканирование localhost 7

3.2 Сканирование localhost/dvwa/ 9

4 Вывод. 11

1 Цель работы

Целью данной работы является изучение сканера уязвимостей nikto.

2.1 Nikto: Описание

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности. Основные задачи Nikto:

• Поиск общих уязвимостей веб-серверов.

• Проверка наличия опасных файлов и конфигураций.

• Выявление устаревших версий веб-серверов и их компонентов.

• Определение серверных технологий и модулей. Особенности:

• Поддержка множества серверов и протоколов (HTTP, HTTPS, HTTP/2 и другие).

• Возможность добавления собственных правил для обнаружения уязвимостей.

• Регулярные обновления базы данных уязвимостей.

Nikto — это пассивный сканер, и он не пытается активно взламывать систему, а только собирает информацию о потенциальных уязвимостях. Рекомендуется использовать Nikto в сочетании с другими инструментами безопасности, такими как Nmap и OpenVAS, для более полного анализа безопасности веб-сервера.

2.2 Полезные параметры и примеры

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе. Сканирование веб-сервера

perl nikto.pl -h

Сканирование определенного порта

perl nikto.pl -h -p

Вывод результатов в файл

perl nikto.pl -h -o output.txt

Дополнительные аргументы:

• -ssl — принудительное использование SSL (HTTPS).

• -no_ssl — игнорирование SSL-сертификатов.

• -Tuning — настройка интенсивности сканирования (например, отключение проверки директорий).

• -Plugins — выбор определенных плагинов для сканирования.

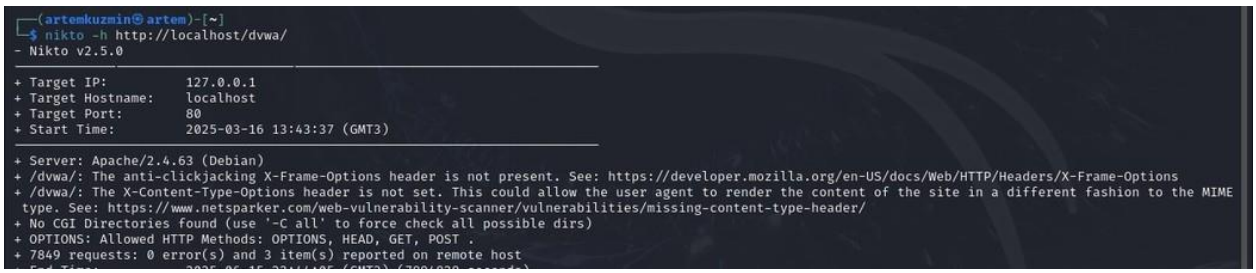
• -timeout — установка таймаута для запросов

3 Выполнение работы

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию. Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

perl nikto.pl -h http://localhost/dvwa/

Рис 1. Тестирование localhost



4 Вывод

В результате выполнения работы я повысил свои навыки использования приложений с целью информационной безопасности. Также познакомился с новым софтом под названием Nikto. Мощные инструменты зайдествованы в этом приложении.